U.S.N | | | | | | | | | | |

P.E.S. College of Engineering, Mandya - 571 401

(An Autonomous Institution affiliated to VTU, Belagavi)

Third Semester, M. Tech - Computer Science and Engineering (MCSE)

Semester End Examination; Dec - 2017/Jan - 2018

Network Security

Time: 3 hrs *Max. Marks: 100*

***Note**: Answer **FIVE** full questions, selecting **ONE** full question from each unit.*

UNIT - I

1	a.	Explain security services and mechanisms.	10
	b.	What is crypto analysis attack? Also discuss different crypto analysis attacks.	10
2	a.	Discuss Rabin Crypto system.	10
	b.	Explain the general structure and analysis of DES.	10

UNIT - II

3	a.	Define Kerberos and name its servers. Briefly explain the duties of each server.	10
	b.	Explain Certification Authority (CA) and its relation to public-key cryptography.	10
4	a.	Compare and contrast key management in PGP and S/MIME.	10
	b.	Explain the Diffie-Hellman and Station-to-Station key agreement.	10

UNIT - III

5	a.	List and explain the parameters that define an SSL session and connections.	10
	b.	Explain different formats of SSL messages.	10
6	a.	Compare and contrast the Handshake protocol and Record protocols in SSL and TLS.	10
	b.	Explain different service and key exchange algorithms of SSL architecture.	10

UNIT - IV

7	a.	Define security policy and explain its purpose with relation to IPsec.	10
	b.	Discuss the two modes of IPsec.	10
8	a.	List ISAKMP payload types and the purpose of each type.	10
	b.	List and define IKE phases and the goal of each phase.	10

UNIT - V

9	a.	Explain how malicious programs exploit the principle of stack overflow for attacking systems?	10
	b.	What is a virus? Explain the differences between worms and viruses.	10
10	a.	List and explain different types of firewalls.	10
	b.	What are the types of analysis adopted by Intrusion Detection and Protection Systems (IDPS)? Discuss the types of IDPS.	10

* * *